ABSTRACT

SEU mitigation, detection, and correction techniques are disclosed. The mitigation techniques include: triple redundancy of a logic path is extended the length of the FPGA to avoid weak points susceptible to SEU effects; triple logic module and feedback redundancy provides redundant hardwired voter circuits at redundant logic outputs and voter circuits in feedback loops to ensure each logic module will receive accurate current state data even if it was upset by an SEU; enhanced triple device redundancy using three FPGAs is introduced, with a fourth device acting as a voting circuit and employing triple logic module and feedback redundancy of the second technique to provide nine instances of the user's logic and ensure complete accuracy in the system; critical redundant outputs are wire-ANDed together to ensure the output is asserted only when the redundant logic modules agree it should be asserted; redundant dual port RAMs are provided, with one port of each RAM dedicated to refreshing data and the remaining port of each RAM being available for use with the user's logic; and redundant clock delay locked loops (DLL) are provided and each DLL is monitored and reset if it does not remain in phase with the majority of the DLLs. The detection techniques include: configuration memory readback wherein a checksum for the expected value is verified; separate FPGAs perform readbacks of configuration memory of a neighbor FPGA; and an FPGA performs a self-readback of its configuration memory array. The correction techniques include reconfiguration of partial configuration data and "scrubbing" based on anticipated rather than actually detected SEUs.